Generalization of Grover's Algorithm to Multiobject Search in Quantum Computing, Part II: General Unitary Transformations

Goong Chen[(1),(2)] and Shunhua Sun[(3)]

Abstract

There are major advantages in a newer version of Grover's quantum algorithm [4] utilizing a general unitary transformation in the search of a single object in a large unsorted database. In this paper, we generalize this algorithm to multiobject search. We show the techniques to achieve the reduction of the problem to one on an invariant subspace of dimension just equal to two.

(1) Department of Mathematics, Texas A&M University, College Station, TX 77843-3368. E-mail: gchen@math.tamu.edu.

(2) Supported in part by Texas A&M University Interdisciplinary Research Initiative IRI 99-22.

(3) Department of Mathematics, Sichuan University, Chengdu, Sichuan, China. Supported in part by a grant from Natural Science Foundation of China.

1 Introduction

This paper is a continuation from [1] on quantum computing algorithms for multiobject search.

L.K. Grover's first papers [2, 3] on "quantum search for a needle in a haystack" have stimulated broad interest in the theoretical development of quantum computing algorithms. Let an unsorted database consist of N objects $\{w_j \mid 1 \le j \le N\}$; each object w_j is stored in a quantum computer (QC) memory as an eigenstate $|w_j\rangle$, $j = 1, 2, \ldots, N$, with $\mathcal{B} \equiv \{|w_j\rangle \mid 1 \le j \le N\}$ forming an orthonormal basis of a Hilbert space $\mathcal{H}$. Let $|w\rangle$ be an element of $\mathcal{B}$ which is the (single) object to be searched. Grover's algorithm in [2, 3] is to utilize a unitary operator

$$U \equiv -I_s I_w \tag{1.1}$$

where

$$I_w \equiv \boldsymbol{I} - 2|w\rangle\langle w|, \qquad (\boldsymbol{I} \equiv \text{ the identity operator on } \mathcal{H}) \tag{1.2}$$

$$I_s \equiv \boldsymbol{I} - 2|s\rangle\langle s|, \qquad |s\rangle \equiv \frac{1}{\sqrt{N}} \sum_{i=1}^{N} |w_i\rangle, \tag{1.3}$$

to perform the iterations $U^m|s\rangle$, which will lead to the target state $|w\rangle$ with probability close to 1 after approximately $\frac{\pi}{4}\sqrt{N}$ number of iterations. The algorithm is of optimal order.

In a more recent paper [4], Grover showed that the state $|s\rangle$ in (1.3) can be replaced by *any* quantum state $|\gamma\rangle$ with nonvanishing amplitude for each object w_j and, correspondingly, the Walsh-Hadamard operator previously used by him to construct the operator I_s can be replaced by a sufficiently general nontrivial unitary operator. Grover's new "search engine" in [4] is a unitary operator taking the form

$$U = -I_\gamma V^{-1} I_w V : \ \mathcal{H} \to \mathcal{H} \tag{1.4}$$

where V is an *arbitrary* unitary operator. The object w will be attained (with probability close to 1) by iterating $U^m|\gamma\rangle$.

This seems to give the algorithm/software designer large flexibility in conducting quantum computer search and code development. It increases the variety of quantum computational operations that can feasibly be performed by practical software. In particular, it opens the possibility of working with an initial state $|\gamma\rangle$ (in place of $|s\rangle$) that is other than a superposition of exactly $N = 2^n$ (n = number of qubits) alternatives. This suggests a new paradigm in which the whole dataset (not just the key) is encoded in the quantum apparatus. This new point of view may also overcome some of the practical difficulties noted by Zalka [6] in searching a physical database by Grover's method.

In the next section, we study the generalization of (1.4) to multiobject search.

2 Multiobject Search Algorithm Using a General Unitary Transformation

Let $\{|w_i\rangle \mid 1 \le i \le N\}$ be the basis of orthonormal eigenstates representing an unsorted database w_i, $1 \le i \le N$, as noted in §I. We inherit much of the notation in [1]: let f be an oracle function such that

$$f(w_i) = \begin{cases} 1, & 1 \le i \le \ell, \\ 0, & \ell+1 \le i \le N, \end{cases}$$

where w_i, $i = 1, 2, \ldots, \ell$, represent the multiobjects under search. We wish to find at least one w_i, for $i = 1, 2, \ldots, \ell$. Let $|\gamma\rangle$ be *any* unit vector in $\mathcal{H}$, and let $L \equiv \operatorname{span}\{|w_i\rangle \mid 1 \le i \le \ell\}$. Define

$$I_\gamma = \boldsymbol{I} - 2|\gamma\rangle\langle\gamma|\colon\ \mathcal{H} \to \mathcal{H},$$

and

$$I_L|w_j\rangle = (-1)^{f(w_j)}|w_j\rangle, \qquad j = 1, 2, \ldots, N,$$

and I_L is then uniquely extended linearly to all $\mathcal{H}$ with the representation

$$I_L = \boldsymbol{I} - 2\sum_{i=1}^{\ell} |w_i\rangle\langle w_i|.$$

Both I_γ and I_L are unitary operators. Let V be any unitary operator on $\mathcal{H}$. Now, define

$$U = -I_\gamma V^{-1} I_L V. \tag{2.1}$$

Then U is a unitary operator; it degenerates into Grover's operator U in (1.4) when $\ell = 1$ and further into the old Grover's operator U in (1.1) if $V \equiv \boldsymbol{I}$.

The unit vector $|\gamma\rangle \in \mathcal{H}$ is arbitrary except that we require $V|\gamma\rangle \notin L$. (Obviously, any $|\gamma\rangle$ such that $\langle w_i|\gamma\rangle \ne 0$ for all $i = 1, 2, \ldots, N$, will work, including $|\gamma\rangle \equiv |s\rangle$ in (1.3).) If $V|\gamma\rangle \in L$, then

$$V|\gamma\rangle = \sum_{j=1}^{\ell} g_i|w_i\rangle, \quad g_i \in \mathbb{C}, \quad \sum_{j=1}^{\ell} |g_i|^2 = 1.$$

A measurement of the state $V|\gamma\rangle$ will yield an eigenstate $|w_j\rangle$, for some $j\colon\ 1 \le j \le \ell$, with probability $|g_j|^2$. Thus the search task would have been completed. Thus, let us consider the nontrivial case $V|\gamma\rangle \notin L$. This implies $|\gamma\rangle \notin V^{-1}(L)$ and, hence,

$$\widetilde{L} \equiv \operatorname{span}(\{|\gamma\rangle\} \cup V^{-1}(L)) \tag{2.2}$$

is an $(\ell+1)$-dimensional subspace of $\mathcal{H}$. It effects a reduction to a lower dimensional invariant subspace for the operator U, according to the following.

Lemma 2.1. *Assume that $\langle\gamma|\gamma\rangle = 1$ and $V|\gamma\rangle \notin L$. Then $U(\widetilde{L}) = \widetilde{L}$.*

Proof. For any $j\colon\ 1 \le j \le \ell$, denote

$$\mu_{\gamma,j} = \langle w_j|V|\gamma\rangle.$$

(1) We have, for $j\colon\ 1 \le j \le \ell$,

$$\begin{aligned}
U(V^{-1}|w_j\rangle) &= -I_\gamma V^{-1}\left(I - 2\sum_{i=1}^{\ell}|w_i\rangle\langle w_i|\right)|w_j\rangle \\
&= -I_\gamma V^{-1}(-|w_j\rangle) \\
&= I_\gamma V^{-1}|w_j\rangle \\
&= (I - 2|\gamma\rangle\langle\gamma|)V^{-1}|w_j\rangle \\
&= V^{-1}|w_j\rangle - 2(\langle\gamma|V^{-1}|w_j\rangle)|\gamma\rangle \\
&= V^{-1}|w_j\rangle - 2\overline{\mu}_{\gamma,j}\gamma \in \widetilde{L}; \qquad (2.3)
\end{aligned}$$

(2)

$$\begin{aligned}
U|\gamma\rangle &= -I_\gamma V^{-1}\left(I - 2\sum_{i=1}^{\ell}|w_i\rangle\langle w_i|\right)(V|\gamma\rangle) \\
&= -(I - 2|\gamma\rangle\langle\gamma|)\left[|\gamma\rangle - 2\sum_{i=1}^{\ell}(\langle w_i|V|\gamma\rangle)V^{-1}|w_i\rangle\right] \\
&= |\gamma\rangle + 2\sum_{i=1}^{\ell}\mu_{\gamma,i}V^{-1}|w_i\rangle - 4\sum_{i=1}^{\ell}\mu_{\gamma,i}\overline{\mu}_{\gamma,i}|\gamma\rangle \\
&= \left(1 - 4\sum_{i=1}^{\ell}|\mu_{\gamma,i}|^2\right)|\gamma\rangle + 2\sum_{i=1}^{\ell}\mu_{\gamma,i}V^{-1}|w_i\rangle \in \widetilde{L}. \quad \square \qquad (2.4)
\end{aligned}$$

By Lemma 2.1, the Hilbert space $\mathcal{H}$ admits an orthogonal direct sum decomposition

$$\mathcal{H} = \widetilde{L} \oplus \widetilde{L}^{\perp}$$

such that $\widetilde{L}^{\perp}$ is also an invariant subspace of U. In our subsequent iterations, the actions of U will be restricted to $\widetilde{L}$, as the following Lemma 2.2 has shown. Therefore we can ignore the complementary summand space $\widetilde{L}^{\perp}$.

Lemma 2.2. *Under the same assumptions as Lemma 2.1, we have $U^m|\gamma\rangle \in \widetilde{L}$ for $m \in \mathbb{Z}^+ \equiv \{0, 1, 2, \dots\}$.*

Proof. It follows obviously from by (2.2) and Lemma 2.1. $\square$

Consider the action of U on $\widetilde{L}$. Even though $|\gamma\rangle, V^{-1}|w_i\rangle$, $i = 1, \dots, \ell$, form a basis of $\widetilde{L}$,

these vectors are not mutually orthogonal. We have

$$U \begin{bmatrix} |\gamma\rangle \\ V^{-1}|w_1\rangle \\ V^{-1}|w_2\rangle \\ \vdots \\ V^{-1}|v_\ell\rangle \end{bmatrix} = \begin{bmatrix} 1-4\sum_{i=1}^{\ell}|\mu_{\gamma,j}|^2 & 2\mu_{\gamma,1} & 2\mu_{\gamma,2} & \dots & 2\mu_{\gamma,\ell} \\ -2\overline{\mu}_{\gamma,1} & 1 & 0 & \dots & 0 \\ -2\overline{\mu}_{\gamma,2} & 0 & 1 & & 0 \\ \vdots & \vdots & & \ddots & \vdots \\ -2\overline{\mu}_{\gamma,\ell} & 0 & 0 & \dots & 1 \end{bmatrix} \begin{bmatrix} |\gamma\rangle \\ V^{-1}|w_1\rangle \\ V^{-1}|w_2\rangle \\ \vdots \\ V^{-1}|w_\ell\rangle \end{bmatrix}, \tag{2.5}$$

$$\equiv \mathcal{M} \begin{bmatrix} |\gamma\rangle \\ V^{-1}|w_1\rangle \\ V^{-1}|w_2\rangle \\ \vdots \\ V^{-1}|w_\ell\rangle \end{bmatrix},$$

according to (2.3) and (2.4). Therefore, with respect to the basis $\{|\gamma\rangle, V^{-1}|w_i\rangle \mid i = 1, \dots, \ell\}$, the matrix representation of U on $\tilde{L}$ is $\mathcal{M}^T$, the transpose of $\mathcal{M}$. These two $(\ell+1)\times(\ell+1)$ matrices $\mathcal{M}$ and $\mathcal{M}^T$ are *nonunitary*, however, because the basis $\{|\gamma\rangle, V^{-1}|w_i\rangle|, i = 1, 2, \dots, \ell\}$ is not orthogonal. This fact is relatively harmless here, as we can further effect a reduction of dimensionality by doing the following. Define a unit vector

$$|\mu\rangle = 2\sum_{j=1}^{\ell} \mu_{\gamma,j} V^{-1}|w_j\rangle / a, \quad a \equiv \left(4\sum_{j=1}^{\ell}|\mu_{\gamma,j}|^2\right)^{1/2} > 0. \tag{2.6}$$

Theorem 2.3. *Let $\mathcal{V} \equiv span\{|\gamma\rangle, |\mu\rangle\}$. Then $\mathcal{V}$ is a two-dimensional invariant subspace of U. We have*

$$U \begin{bmatrix} |\gamma\rangle \\ |\mu\rangle \end{bmatrix} = M \begin{bmatrix} |\gamma\rangle \\ |\mu\rangle \end{bmatrix}, \qquad M \equiv \begin{bmatrix} 1-a^2 & a \\ -a & 1 \end{bmatrix}. \tag{2.7}$$

Consequently, with respect to the basis $\{|\gamma\rangle, |\mu\rangle\}$ in $\mathcal{V}$, the matrix representation of U is M^T.

Proof. Using (2.3), we have

$$\begin{aligned} U|\mu\rangle &= 2\sum_{j=1}^{\ell} \mu_{\gamma,j} V^{-1}|w_j\rangle \cdot \frac{1}{a} - 2\sum_{j=1}^{\ell} |\mu_{\gamma,j}|^2 \cdot \frac{1}{a}|\gamma\rangle \\ &= |\mu\rangle - a|\gamma\rangle. \end{aligned}$$

Again, from the definition of $|\mu\rangle$ in (2.6), we see that (2.4) gives

$$U|\gamma\rangle = (1-a^2)|\gamma\rangle + a|\mu\rangle.$$

Therefore (2.7) follows. □

Theorem 2.3 gives a dramatic reduction of dimensionality to **2**, i.e., the dimension of the invariant subspace $\mathcal{V}$. Again, we note that the matrices M and M^T in (2.7) are *not unitary*.

Any vector $|v\rangle \in \mathcal{V}$ can be represented as

$$|v\rangle = c_1|\gamma\rangle + c_2|\mu\rangle,$$

and so

$$U|v\rangle = U(c_1|\gamma\rangle + c_2|\mu\rangle$$
$$= c_1[(1-a^2)|\gamma\rangle + a|\mu\rangle] + c_2[-a|\gamma\rangle + |\mu\rangle],$$

and thus

$$U|v\rangle = M^T \begin{bmatrix} c_1 \\ c_2 \end{bmatrix} = \begin{bmatrix} 1-a^2 & -a \\ a & 1 \end{bmatrix} \begin{bmatrix} c_1 \\ c_2 \end{bmatrix}, \tag{2.8}$$

where the first component of the vector on the right hand side of (2.8) corresponds to the coefficient of $|\gamma\rangle$ while the second component corresponds to the coefficient of $|\mu\rangle$. Therefore

$$U^m|\gamma\rangle = \begin{bmatrix} 1-a^2 & -a \\ a & 1 \end{bmatrix}^m \begin{bmatrix} 1 \\ 0 \end{bmatrix}. \tag{2.9}$$

The above can be viewed geometrically ([5]) as follows:

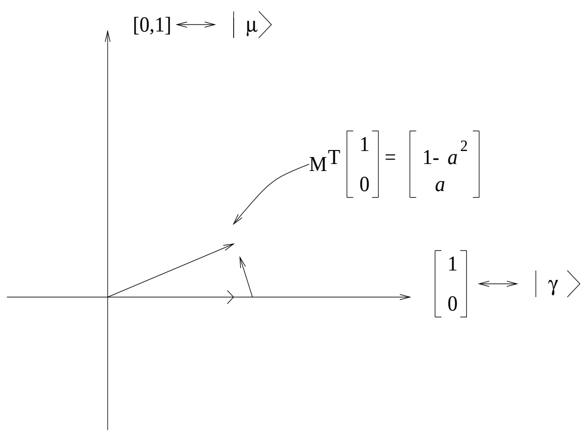

Figure 2.1: A geometric view of a single iteration (2.8)

$M^T \left[\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right] = \left[\begin{smallmatrix} 1-a^2 \\ a \end{smallmatrix}\right]$, for $a > 0$ very small, $a \approx \sin a$, and therefore $\left[\begin{smallmatrix} 1-a^2 \\ a \end{smallmatrix}\right]$ is a vector obtained from the unit vector $\left[\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right]$ by rotating it counterclockwise with angle a. It takes approximately

$$m \approx \frac{\pi/2}{a} = \frac{\pi}{2a} = \pi \Big/ 4 \left[\sum_{j=1}^{\ell} |\mu_{\gamma,j}|^2 \right]^{1/2}$$

rotations to closely align the vector $U^m|\gamma\rangle$ with $|\mu\rangle \in V^{-1}L^1$. Thus $V(U^m|\gamma\rangle)$ deviates little from the subspace $L = \text{span}\{|w_i\rangle \mid i = 1, 2, \ldots, \ell\}$. A measurement of $VU^m|\gamma\rangle$ gives one of the eigenstates $|w_j\rangle$, for some j: $1 \le j \le \ell$, with probability nearly equal to 1, and the task of multiobject search is completed with this large probability.

References

[1] G. Chen, S.A. Fulling and M.O. Scully, Generalization of Grover's algorithm to multiobject search in quantum computing, Part I: Continuous time and discrete time, preprint.

[2] L.K. Grover, A fast quantum mechanical algorithm for database search, Proc. 28th Annual Symposium on the Theory of Computing, 212–218, ACM Press, New York, 1996.

[3] L.K. Grover, Quantum mechanics helps in searching for a needle in a haystack, Phys. Rev. Letters **78** (1997), 325–328.

[4] L.K. Grover, Quantum computers can search rapidly by using almost any transformation, Phys. Rev. Letters **80** (1998), 4329–4332.

[5] R. Jozsa, Searching in Grover's algorithm, `quant-ph/9901021`, Jan. 1999.

[6] C. Zalka, Could Grover's quantum algorithm help in searching an actual database? `quant-ph/9901068`, Jan. 1999.